Web Images Video News Maps **more »**

TPM hypervisor TCPA Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

Scholar **All articles** - **Recent articles** Results **1** - **10** of about **37** **English** pages for **TPM hypervisor TCPA**. (**0.24** seconds)

[PDF] Trusted linux client
D Safford, M Zohar - IBM TJ Watson Research Center, 2004 - acsac.org
... http://www.research.ibm.com/gsal/**tcpa** device driver/access library/example applications Bottom line: **...** **TPM** Secure **Hypervisor** Trusted Platform Module Trusted **...**
Cited by 3 - Related articles - View as HTML - Web Search - All 2 versions

Para-Virtualized **TPM** Sharing
P England, J Loeser - Trusted Computing Challenges and Applications: First ..., 2008 - books.google.com
... 845 Guest Measurement 274 Misc (**hypervisor** glue, libc **...** 2004) 3. Goldman, KA, Berger, S.: **TPM** Main Part 3 **...** et al.: Trusted Computing Platforms: **TCPA** Technology in **...**
Web Search

Trusted Code Remote Execution through Trusted Computing and Virtualization
L Zhang, L Chen, H Zhang, F Yan - ... Intelligence, Networking, and Parallel/Distributed Computing ..., 2007 - ieeexplore.ieee.org
... They implement the resources control in Xen **hypervisor** and a **...** MAC policy which under control of **TPM** so we **...** the Trusted Computing Platform Alliance (**TCPA**) in 1999 **...**
Cited by 1 - Related articles - Web Search - All 4 versions

TPM Virtualization: Building a General Framework
V Scarlata, C Rozas, M Wiseman, D Grawrock, C ... - Trusted Computing: Ein Weg zu neuen It- ..., 2007 - books.google.com
... The Software is integrated into **hypervisor** environment in order to **...** org/specs/**TPM**/ [14] Trusted Computing Group **...** Experimenting with **tcpa**/tcg hard- ware, or: How i **...**
Cited by 2 - Related articles - Web Search

TPM Virtualization: Building a General Framework
VSCRM Wiseman, DGC Vishik - Trusted Computing: Ein Weg zu neuen It- ..., 2007 - books.google.com
... The software is integrated into **hypervisor** environment in order to **...** org/specs/**TPM**/ [14] Trusted Computing Group **...** Experimenting with **tcpa**/tcg hard- ware, or: How i **...**
Related articles - Web Search

TPM Virtualization: Building a General Framework
VSC Rozas, M Wiseman, DGC Vishik - Springer
... The software is integrated into **hypervisor** environment in **...** www.trustedcomputinggroup. org/specs/**TPM**/ Trusted Computing **...** Experimenting with **tcpa**/tcg hard- ware, or **...**
Related articles - Web Search

Security Architecture for Device Encryption and VPN
A Alkassar, M Scheibel, C Stüble, AR Sadeghi, M ... - Securing Electronic Business Processes Highlights of the ..., 2006 - Springer
... software layer builds on the **hypervisor** layer and **...** The **TPM** then signs its internal integrity measurements **...** open-source virtual secure coprocessor based on **tcpa**. **...**
Cited by 2 - Related articles - Web Search - All 3 versions

Practical Techniques for Operating System Attestation
P England - Trusted Computing Challenges and Applications: First ..., 2008 - books.google.com
... The authorized **hypervisor** (or hypervisors) is able to **...** J., England, P.: Para-virtualized **tpm** sharing **...** Pearson, S.: Trusted Computing Platforms: **TCPA** Technology in **...**

Web Search

[PDF] Attestation evidence and trust

J Sheehy, G Coker, J Guttman, P Loscocco, A Herzog ... - mitre-corp.org

... the other has a valid unrevoked **TPM** AIK **...** use for separation purposes instead of a traditional **hypervisor**. **...** Trusted Computing Platforms: **TCPA** Technology in Context **...**

Cited by 2 - Related articles - Web Search - All 2 versions

Trusted Computing-Special Aspects and Challenges

A Sadeghi - LECTURE NOTES IN COMPUTER SCIENCE, 2008 - Springer

... GVTPM [39] is a virtual **TPM** framework that supports various **TPM** models and even different security profiles for each VM under the Xen **hypervisor**. **...**

Cited by 5 - Related articles - Web Search - BL Direct - All 2 versions

Key authors: **B Kauer** - **A Sadeghi** - **L Chen** - **G Proudler** - **R Landfermann**

Goooogle ▶

Result Page: 1 2 3 4 **Next**

TPM hypervisor TCPA | Search

Google Home - About Google - About Google Scholar